# TRUDEVICE WORKSHOP 2015 – Program (tentative)

| | |
|---|---|
| **8:30 – 8:45** | **Opening session** |
| **8:45 – 9:30** | **Keynote** |
| | ***The pros and cons of technological dispersion for security: PUF, TRNG and side-channel countermeasures***<br>Jean-Luc Danger |
| **9:30 – 10:30** | **Session 1 (4 Papers)** |
| | ***Analysis and utilization of deviations in RO-PUFs under altered FPGA designs***<br>Linus Feiten, Tobias Martin, Bernd Becker<br><br>***Ring Oscillators Analysis for FPGA Security Purposes***<br>Mario Barbareschi, Lionel Torres, Giorgio Di Natale<br><br>***Enhanced TERO-PUF design and characterization with FPGA***<br>Cedric Marchand, Abdelkarim Cherkaoui, Lilian Bossuet<br><br>***Implementing Reliable Mechanisms for IP Protection on Low-End FPGA devices***<br>Mario Barbareschi, Antonio Mazzea, Pierpaolo Bagnasco |
| **10:30 – 11:30** | **Coffee break (and poster session 1)** |
| **11:30 – 12:00** | **Session 2 (2 Papers)** |
| | ***Hierarchical Secure DfT.***<br>Mafalda Cortez, Said Hamdioui, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre<br><br>***Integrated Sensors: A Backdoor for Hardware Trojan Activation***<br>Xuan-Thuy Ngo, Zakaria Najm, Shivam Bhasin, Sylvain Guilley, Jean-Luc Danger |
| **12:00 – 13:00** | **Lunch** |
| **13:00 – 13:45** | **Keynote 2** |
| | ***Protecting Cryptographic Implementations on Reconfigurable Devices***<br>Tim Güneysu |
| **13:45 – 14:45** | **Session 3 (4 Papers)** |
| | ***Towards Generic Countermeasures Against Fault Injection Attacks.***<br>Pablo Rauzy, Sylvain Guillet<br><br>***Analysis of laser-induced errors: RTL fault model versus layout locality characteristics.***<br>Anthanasios Papadimitriou, David Hely, Vincent Beroulle, Paolo Maistri, Regis Leveugle<br><br>***Sensitivity to fault laser injection: a comparison between 28nm bulk and FD-SOI technology***<br>Stephan DeCastro, Giorgio Di Natale<br><br>***Dynamic Fault Model for Long Duration Laser-Induced Fault Simulation.***<br>Feng Lu, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre |
| **14:30 – 15:00** | **Coffee break (and poster session 2)** |
| **15:00 – 15:45** | **Session 4 (3 Papers)** |
| | ***Public Key cryptographic primitive design and protection against fault and power analysis attacks.***<br>Apostolos P. Fournaris, Nicolas Sklavos<br><br>***On the Use of Error Detecting and Correcting Codes to Boost Security in Caches against Side Channel Attacks.***<br>Madalin Neagu, Slavador Manich, Liviu Miclea<br><br>***A Side-Channel Attack Against Secret Permutation on an Embedded McEliece Cryptosystem.***<br>Tania Richmond, Martin Petrvalsky, Milos Drutarovsky |
| **15:45 – 16:45** | **Session 5 (4 Papers)** |

| | |
|---|---|
| | ***Investigating TERO for Hardware Trojan Horse Detection.***<br>Paris Kitsos, Artemios G. Voyiatzis<br><br>***Insertion and evaluation of Hardware Trojans in Processors***<br>I. Voyiatzis, C. Efstathiou, Th. Milidonis<br><br>***Security of ICs from Hardware Trojans.***<br>Georgina Kalogeridou, Nicolas Sklavos, Andrew W. Moore, Odysseas Koufopaulou<br><br>***HINT: Holistic Approaches for Integrity of ICT-Systems.***<br>Ingrid Verbauwhede, Dave Singelee |
| **16:45 – 17:00** | **Closing session** |

# Poster Session 1 (Morning)

***Functional Locking Modules for Design Protection of Intellectual Property Cores***
Brice Colombier, Lilian Bossuet

***3D-NoC protection capabilities and threats: The TSV risk***
Johanna Sepulveda, Guy Gogniat, Marius Strum

***Hardware Trojans in TRNGs***
Honorio Martin, Pedro Paris-Lopez, Enrique San Millan, Juan E. Tapidor, Nicolas Sklavos

***Development of a Layout-Level Hardware Obfuscation Tool***
Shweta Malik, Georg T. Becker, Christof Paar, Wayne P. Burleson

***GET - Program for the Generation and Analysis on Nonlinear Elements***
Stjepan Picek, Lejla Batina

***Why you should care about leading-edge Software Engineering?***
Tiziana Margaria

***Error detection and correction for lightweight cryptographic algorithms.***
Francesco Regazzoni, Andrey Bogdanov, Luca Breveglieri, Israel Koren

***Fine grain partial reconfiguration for fault emulation and precise LUT modification.***
L.A. Cardona,B. Lorente,C. Ferrer

# Poster Session 2 (Afternoon)

***A Novel Scheduling Policy for Thwarting Differential Power Analysis Attacks.***
Ke Jiang

***Exploring RNS in the design of improved RSA implementations.***
Juvenal Araujo, Pedro Matutino, Leonel Sousa, Ricardo Chaves

***CAESAR and NORX – Developing the Future of Authenticated Encryption.***
Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves

***Power and Electromagnetic Analysis for Online Template Attacks***
Margaux Dugardin, Louiza Papchristodoulou, Zakaria Najm, Lejla Batina, Jean-Luc Danger, Sylvain Guilley, Jean-Christophe Courrège, Anne-Sophie Rivemale, and Carine Therond

***Search Strategy for Fault Injection using Memetic Algorithms***
Stjepan Picek, Pieter Buzing,Lejla Batina

***Insights into the Correlation between the Processed Data and its Power Traces***
Miryam Haber, Binyamin Frankel, Moshe Avital, Itamar Levi, Osnat Keren, Alexander Fisch

***Tuning of randomized windows against simple power analysis for scalar multiplication on elliptic curves.***
Simon Pontie, Paolo Maistri and Regis Leveugle